UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA, Plaintiff, v. MARCUS A. OWENS, Defendant.	Case No. 16-CR-38-JPS **ORDER**

Before the Court is Defendant Marcus A. Owens' ("Owens") objection to Magistrate Judge David E. Jones' order of November 4, 2016, denying his motion to compel discovery regarding the "Network Investigative Technique" ("NIT") employed by the government in this case. For the reasons stated below, Magistrate Jones' ruling will be affirmed in its entirety.

1. BACKGROUND[1]

1.1 Playpen Investigation

In late 2014, the FBI began investigating Playpen, a website used to advertise and distribute child pornography. (Docket #78 at 2). The website was accessible to Internet users through a "Tor" browser, which masks the user's Internet Protocol ("IP") address and, as a result, his identity. *Id.* The FBI apprehended the administrator of the Playpen site in early 2015 and thereafter allowed Playpen to continue operating on a server located in a government facility in the Eastern District of Virginia. *Id.*

[1]Owens offers no specific objections to any of the facts as stated by Magistrate Jones. Accordingly, the Court adopts those factual findings and incorporates them in summary fashion here.

On February 20, 2015, a United States magistrate judge sitting in the Eastern District of Virginia issued a warrant authorizing the government to deploy an NIT on that server. *Id.* at 2–3. The NIT was able to function because it exploited a vulnerability in the Tor browser through which it could access activating computers. *Id.* at 6. In addition to the normal content the end user downloaded from the Playpen site, the NIT downloaded additional instructions onto the end user's computer. *Id.* at 3. For purposes of the NIT warrant, the end user's computer was dubbed the "activating computer." *Id.* After downloading the additional instructions, the activating computer would transmit certain content-neutral identifying information to the government-controlled server. *Id.* The NIT was deployed each time a user logged onto Playpen while it was under government control, which lasted from February 20 to March 4, 2015. *Id.* According to the government, the NIT did not reveal any information other than the identifying data listed in the warrant and it did not deny the user access to any data on or functionality of his computer. *Id.*

While operating Playpen in conjunction with the NIT, the FBI identified Owens as a Playpen user. *Id.* Law enforcement officers subsequently obtained a warrant to search Owens' home. *Id.* Upon executing the warrant, officers recovered an external hard drive that contained numerous images and videos of suspected child pornography. *Id.* at 4. Owens agreed to speak with law enforcement and he admitted accessing certain websites that contained images of child pornography. *Id.* Based on the evidence seized from the residence and his statement to law enforcement, Owens was arrested pursuant to a criminal complaint that charged him with receiving and possessing child pornography. (Docket #1). On March 1, 2016, a grand jury returned an indictment against Owens, charging him with one

count of knowingly receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and one count of knowingly possessing matter that contained images of child pornography, in violation of 18 U.S.C. § 2252A(a)(5). (Docket #9).

1.2 Owens' Motion to Compel

On March 24, 2016, Owens wrote a letter to the government requesting that it produce "a complete copy of the code used for the NIT." (Docket #76-3). The government agreed to produce only a portion of the NIT's source code. Thereafter, Owens retained Matthew Miller ("Dr. Miller"), an assistant professor of computer science and information technology at the University of Nebraska at Kearney, to analyze the portion of the NIT code the government produced. (Docket #78 at 4–5). Dr. Miller opined that he needed to evaluate additional portions of the NIT that the government had not produced. (Docket #76-1). The government agreed to produce some additional information but again stopped short of producing everything Owens requested. (Docket #68). Owens filed a motion to compel the entire NIT source code on November 1, 2016. (Docket #76).

The NIT, according to Owens, has four discrete components: (1) tracking server software used to generate and track the information extracted from activating computers; (2) exploit software used to take advantage of a software flaw in the Tor browser; (3) payload software that ran on the activating computers to extract information and report that information back to the government server; and (4) collection server software that stored the extracted information on the government server. (Docket #62 at 2). To date, the government has produced the tracking server software and the payload software. *Id.* at 4. Owens still seeks the exploit software, a "human-readable" form of the payload software, and the collection server software. *Id.*

In litigating the matter before Magistrate Jones, Owens offered two rationales for his need to discover these additional pieces of the NIT source code. First, Owens suspects that the NIT "may have extracted more information from his computer than the warrant permitted." *Id.* at 5. Second, Owens contends that "the NIT's exploit component may have altered [his] computer, potentially creating an ongoing vulnerability for attack by a third party—that is, it may have allowed a third party to use the computer and store information on it, including the illegal material now being attributed to him." *Id.*

As an initial matter, the government argued that it had produced what it believed to be the entire source code for the NIT—that is, the additional instructions the NIT downloaded on the activating computers in addition to Playpen's usual content. (Docket #70-2 ¶ 5). On top of that, the government has made Owens' computer available to him and produced the two-way data stream showing what information went into Owens' computer and what information was sent back to the government-hosted computer server. *Id.* ¶ 15; (Docket #78 at 8). According to the government, Dr. Miller has analyzed the data stream and has confirmed that this information matches the NIT results. (Docket #78 at 8); (Docket #76-1 ¶ 2).

Further, says the government, even if the NIT could be separated into components as Owens requests, it should not be required to produce those components. First, there is no "human-readable" form of the payload software, and second, the exploit and collection server software are immaterial to Owens' defense and are subject to the law enforcement privilege. *Id.* On this second point, the government viewed Owens' rationales for the materiality of the software as mere supposition, unsupported by any evidence that the government actually extracted more information from his

computer than authorized or left his computer open to third-party attack. *Id.* at 8–9.

1.3 Magistrate Jones' Order

Magistrate Jones heard oral argument and took several submissions from both sides regarding Owens' motion to compel. (Docket #68, #70, #71, #72, #76, and #77). On November 4, 2016, Magistrate Jones issued a decision denying the motion. (Docket #78).

Magistrate Jones rejected Owens' proffered theories as to the materiality of the remainder of the NIT source code. *Id.* at 9. Magistrate Jones labeled Owens' arguments "speculation concerning what the NIT might have done" which lacked supporting evidence. *Id.* Further, Magistrate Jones concluded that although Dr. Miller believes he needs more of the NIT source code for his analyses, he failed to explain why other than to simply repeatedly say that he needs it. *Id.* Magistrate Jones concluded that Owens' arguments failed to meet his *prima facie* burden under Federal Rule of Criminal Procedure 16(a) to support an order compelling further disclosure from the government. *Id.* at 9–10.

In particular, Magistrate Jones explained that Dr. Miller could resolve whether the NIT took more information than the warrant described by running the NIT payload component, which the government has produced, on Owens' computer. *Id.* at 10. Moreover, Owens offered no evidence that the government lied in the NIT warrant application when it stated that the NIT would extract no more information than those items identified in the warrant. *Id.*

Additionally, Magistrate Jones found unavailing Owens' contention that the NIT left his computer open to third-party attackers, who might have exploited a vulnerability created by the NIT to place images of child

pornography on his computer. *Id.* at 11. Magistrate Jones was "deeply skeptical of such chicanery," particularly since Owens pointed only to a few newspaper articles describing unrelated past instances in which such conduct occurred. *Id.* More pertinent to the instant case, in Magistrate Jones' view, was the fact that Owens' theory "does nothing to discredit the fact that [Owens] downloaded child pornography while visiting Playpen, and had child pornography on hard drives that were detached from his computer." *Id.* (internal citation omitted).

Magistrate Jones drew a similar conclusion with respect to the collection server software. The NIT "appears to have taken only one second" to extract data from Owens' computer, reducing the likelihood that the information it collected was accessed by third parties in transit to the government's server. *Id.* Moreover, Owens can test the reliability of the data extracted from his computer since he now has access to the two-way data stream and his computer. *Id.*

Finally, Magistrate Jones found that Owens failed to show why he needs that exploit software. *Id.* Again, because he can examine his own computer, Magistrate Jones found that Owens has the ability to determine whether the NIT manipulated his security settings, leaving him vulnerable to outside attack. *Id.* Similarly, he can test the NIT on his or another computer to see if it does in fact change any security settings. *Id.* Although Owens complained that the NIT—which he labels "malware"—would likely not leave a trace of its presence on his computer, he had failed, according to Magistrate Jones, to undertake "any intermediate steps to test [his] hypotheses. . . . Without any such tests, the defense has only a theory unsupported by fact." *Id.* at 12.

Owens timely objected to Magistrate Jones' ruling. (Docket #81). The government responded to the objections. (Docket #82). Owens did not file a reply, and the deadline to do so has expired. His objections are, therefore, ripe for disposition.

2. STANDARD OF REVIEW

2.1 Review of a Magistrate Judges' Non-Dispositive Order

Federal Rule of Criminal Procedure 59(a) governs the district court's review of a magistrate judge's ruling on a non-dispositive matter, such as Owens' motion to compel discovery. Parties have fourteen days to file "specific written objections" to a magistrate judge's non-dispositive pretrial order. Fed. R. Crim. P. 59(a). When reviewing the magistrate judge's order, the Court is obliged to analyze any timely objections and must "modify or set aside any part of the order that is contrary to law or clearly erroneous." *Id.*

2.2 The Scope of Criminal Discovery Under Rule 16

Discovery matters in criminal cases are committed to the sound discretion of the trial court. *United States v. Bastanipour*, 697 F.2d 170, 175 (7th Cir. 1982). Rule 16(a) of the Federal Rules of Criminal Procedure sets forth the narrow grounds upon which a criminal defendant may demand discovery from the government. The Rule provides, in relevant part, that the government must produce upon request documents and data if they are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E)(I). Materiality in this context means that the discovery sought must "significantly hel[p] in 'uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment and rebuttal.'" *United States v. Gaddis*, 877 F.2d 605, 611 (7th Cir. 1989) (quoting *United States v. Felt*, 491 F. Supp. 179, 186 (D.D.C. 1979)). The Seventh Circuit has also described material evidence as that which will "'enable the accused

to substantially alter the quantum of proof in his favor.'" *United States v. Orzechowski*, 547 F.2d 978, 984 (7th Cir. 1976) (quoting *United States v. Marshall*, 532 F.2d 1279, 1285 (9th Cir. 1976)); *United States v. Farah*, 475 F. App'x 1, 6 (4th Cir. 2007) (in contrast to the "relevance" standard used in civil cases, "materiality" means more than "bear[ing] some abstract logical relationship" to the issues in the case; rather, "there must be some indication that the disclosure of the disputed evidence would have enabled the defendant to significantly alter the quantum of proof in his favor").

The defendant bears the burden to "make at least a *prima facie* showing that the requested items are material to his defense." *United States v. Thompson*, 944 F.2d 1331, 1342 (7th Cir. 1991). To do this, "a defendant cannot rely on general descriptions or conclusory arguments" but must instead "convincingly explain how specific documents will significantly help him uncover admissible evidence, prepare witnesses, or corroborate, impeach, or rebut testimony." *United States v. Caputo*, 373 F. Supp. 2d 789, 793 (N.D. Ill. 2005) (collecting cases). Additionally, the district court should "consider the materials that have already been produced, the availability of the requested materials from other sources, and the defendant's own knowledge." *Id.* at 794 (citing *United States v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975)).

3. ANALYSIS

Owens' objections largely rehash the arguments Magistrate Jones rejected, and this Court is obliged to reject them for the same reasons. First, Owens asserts that "what the NIT actually did and how it affected [his] computer is unknown." (Docket #81 at 4). Second, he claims that his computer was left open to third-party attack because the government waited a year to seize his computer after first executing the NIT against it. *Id.*

The Court finds that Owens has not made a showing of materiality sufficient to obtain the discovery he seeks. In so doing, the Court joins the majority of other courts to speak on this issue. *See United States v. Jean*, Case No. 5:15-CR-50087-001, 2016 WL 6886871, at *7 (W.D. Ark. Nov. 22, 2016); *United States v. Matish*, Criminal No. 4:16cr16, 2016 WL 3545776, at *7 (E.D. Va. June 23, 2016); *United States v. McLamb*, CRIMINAL NO. 2:16cr92, 2016 WL 6963046, at *8 (E.D. Va. Nov. 28, 2016); *United States v. Darby*, Criminal No. 2:16cr36, at 8–12 (E.D. Va. Aug. 12, 2016), submitted at (Docket #70-4); *but see United States v. Michaud*, Case No. 3:15-cr-05351-RJB, at 17–22 (W.D. Wash. May 25, 2016) (finding the full source code to be "central to the case" and suppressing all evidence derived from the NIT), submitted at (Docket #76-4).

First, Owens argues that he needs the entire NIT source code to determine whether the NIT operated as the government indicated it would in its warrant application. He notes that the NIT warrant did not permit the government to extract more information than those items listed in the warrant, nor did it permit the government to change security settings on his computer. (Docket #81 at 5). He argues that without access to the exploit component of the NIT, he will have no way to determine "how the NIT affected his device." *Id.*

However, Owens already has the ability to learn what the NIT did to his computer because he has access to the computer itself. He can examine it to evaluate what data or settings, if any, the NIT changed. Additionally, the government has given him access to the payload component of the NIT, allowing him to run that component on his or another computer to observe what it does in practice. Indeed, Dr. Miller appears to have already tested some portions of the NIT he has been provided, and, according to the government, he concluded that the program operated consistently with the

government's representations. Finally, the government has provided the two-way data stream created by the exploit component, thus revealing all the data that passed between his and the government's computer. Consequently, as the district court found in *McLamb*, here "the extent of the information seized from [Owens'] computer is already available to [him], because the information itself has already been disclosed to him." *McLamb*, 2016 WL 6963046, at *8. If the materials Owens has been provided are not enough for him to analyze these issues, he does not explain why, and the Court will not invent such arguments for him. Just as in *Matish*, here "the defense lacks any evidence to support [its] hypotheses and instead relies upon the *ipse dixit* that the source code is needed because its declarants opine that it is needed. Such speculation remains insufficient to serve as a basis to compel discovery." *Matish*, 2016 WL 3545776, at *6.

Because of the breadth of the government's production thus far, this case is unlike *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), cited by Owens. There, a defendant was totally denied access to the specialized peer-to-peer software the government used to download files from his computer. *Id.* at 1112. By contrast, here Owens has been provided with the relevant portions of the NIT and he offers no more than speculation that he requires the remainder. Because his expert, Dr. Miller, can use the parts of the NIT he has to test Owens' hypotheses, his situation is a far cry from *Budziak*, where the defendant had no such opportunity. In short, Owens has the tools at his disposal to test the government's assertions about the operation of the NIT and need not, as he suggests, "take the government's word for it." (Docket #81 at 5).

Second, Owens claims that he cannot evaluate the government's chain of custody of his data without the collection server software. (Docket #81 at

5). Again, given the materials produced to date, this is in fact a question that Owens has the power to answer, since he can analyze the two-way data stream, which reveals what data left his computer and what data arrived at the government's computer. Moreover, as Magistrate Jones observed, the NIT's entire extraction process took about one second, so "it is highly unlikely that the information was tampered with while in transit." (Docket #78 at 11); *Matish*, 2016 WL 3545776, at *7.

Third, Owens complains that without the entire NIT source code, he cannot evaluate whether third-party hacking occurred, which might bear on both his defense and sentencing. (Docket #81 at 6–7). As he did before Magistrate Jones, Owens here relies on a smattering of news coverage regarding years-old schemes to plant child pornography on innocent users' computers. *Id.* at 6. He further asserts that because he visited "questionable corners of the internet (where one's device might attract viruses or other malevolent attention)," his fear of hacking is well-founded. *Id.* at 7.

The Court does not agree. Owens' citations fall well short of showing that there is any non-speculative possibility that he was the victim of such a plot. Owens' third-party hacking theory, like his other rationales, suffers from a complete lack of corroboration. As in the other NIT cases, here the Court has no expert analysis indicating that Owens' theory has any factual basis. *Jean*, 2016 WL 6886871, at *6 (finding that no defense expert "had bothered to examine Mr. Jean's computer to determine whether the exploit did, in fact, disable a firewall or make either a temporary or permanent change to the operating system that could have been detected"); *Matish*, 2016 WL 3545776, at *7 (observing that the defendant failed to perform his own analyses of his computer, which was available to him, to determine if the NIT affected any security settings or programs). It is not enough for him to say

merely that hacking could have occurred, for this does not convincingly explain how his requested discovery would significantly help him develop his defense. *Caputo*, 373 F. Supp. 2d at 793; *Gaddis*, 877 F.2d at 611.

The available evidence, moreover, undermines Owens' hacking theory. Owens admitted that he had accessed websites containing child pornography, and the government located child pornography on Owens' hard drives that were not connected to his computer and thus not interfered with or made vulnerable by the NIT. Additionally, his expert, Dr. Miller, admitted to the court in *Jean* that the likelihood of an outside hacker being responsible for the defendant's child pornography collection was, at best, "very unlikely." *Jean*, 2016 WL 6886871, at *6. In the view of FBI Special Agent Alfin, who testified for the government in *Jean*, the notion that a hacker knew of the Tor browser's vulnerability, hijacked the NIT's exploit component while it was being deployed, and then used it to download his own child pornography onto the activating computer, was "a far-fetched theoretical possibility." *Id.* As the court in *Jean* observed, "simply knowing how the exploit picked the lock would not materially assist the defense in better understanding the relative plausibility of a third-party hacking defense. Regardless of what Dr. Miller might learn from the exploit code, the third-party hacker defense would still be predicated on the simultaneous existence of a long string of hypothetical circumstances." *Id.* Like *Jean*, here the Court cannot order further discovery based on Owens' "virtually impossible hypothetical situation." *Id.*

Owens argues to this Court that his hacking theory is sound because the government's case is tied to six specific images of child pornography identified in the indictment. (Docket #81 at 7). Asserting that "the magistrate judge seemed to miss this point," Owens claims that if his computer "was left

vulnerable by the government's NIT, and was utilized by hackers for nefarious purposes (as were millions of other internet-accessible devices just last month), then this information would certainly seem to create a viable defense—that these six specific files could have been put there by some other entity." *Id.* It is Owens, however, who misses the point, since in his objections he does nothing to cure the evidentiary deficiency which led Magistrate Jones to deny his motion to compel. His vague conjecture about the dangers of hacking does no more to suggest that the six images identified in the indictment were placed on his computer by hackers than any other image on that computer.[2]

Owens makes one final attempt to save his hacking theory, noting that because "[n]early a year passed between the NIT search and the FBI's physical seizure of his computer," his computer was left vulnerable to hackers for a very long time. *Id.* at 7–8. According to Owens, the only way to determine whether the NIT left his computer "unlocked" and open to attack is to examine the program in full. *Id.* at 8. In his opinion, "just looking at his device will not answer whether it has been hacked or not," since hackers often leave no trace of their intrusions. *Id.*

---

[2]And his argument is wrong on a more fundamental level, since the indictment does not limit his charges to those six specific images but merely lists them as exemplars. *See United States v. Traweek*, Criminal Action No. 4:13–CR–712, 2015 WL 5972461, at *17 (S.D. Tex. Oct. 14, 2015) (rejecting the defendant's argument that the government's reliance at trial on images of child pornography not mentioned in the indictment constituted an impermissible constructive amendment of the indictment); *United States v. Cameron*, 662 F. Supp. 2d 177, 180 (D. Me. 2009) (finding that the government need not identify specific images of child pornography in an indictment to comply with the statute or any rule of criminal procedure).

This assertion is simply untrue, for, as other courts have found, Owens could have performed some analyses or simulations on his own computer, or a different computer, to try and substantiate his claims about what the NIT did. He declined to perform these tests and, as a result, his claims have no evidentiary basis. *Matish*, 2016 WL 3545776, at *7 ("[A]n examination of Defendant's computer may have uncovered evidence either of hacking or an alternate source of the child pornography, but, as it stands, the declarants' inaction leaves their hypotheses with no evidence to support them."). Thus, "the defense has failed to advance the speculative hypotheses of its declarants to the realm of significantly altering the quantum of proof." *Id.* at *8; *McLamb*, 2016 WL 6963046, at *8 ("[T]he Defendant knows what was in his computer and the government has offered to let the Defendant examine his computer for signs of hacking. Again, the Defendant has not taken advantage of this offer, and has presented no evidence that his computer was hacked."). As the court in *Darby* put it,"Defendant invents a variety of scenarios" in which the NIT source code would be relevant but he "has not used any of the information that the government has provided to him or offered to provide him in order to establish a factual basis for these scenarios. . . . [A]ll Defendant places before the Court are stories about how a generic defendant located by means of a generic NIT might need the information sought in order to develop his or her defense." *Darby*, (Docket #70-4 at 8). Owens has, therefore, failed to meet his *prima facie* burden to demonstrate that the discovery he seeks is material, and the Court must affirm Magistrate Jones' order denying his discovery requests.[3]

[3]Magistrate Jones analyzed only materiality and did not address the government's claim of law enforcement privilege. Because this Court will affirm Magistrate Jones' order in full, it does not reach the privilege either.

4. CONCLUSION

Owens has not shown that Magistrate Jones' ruling denying his motion to compel was clearly erroneous or contrary to law. As a result, for the reasons stated above, it must be affirmed.

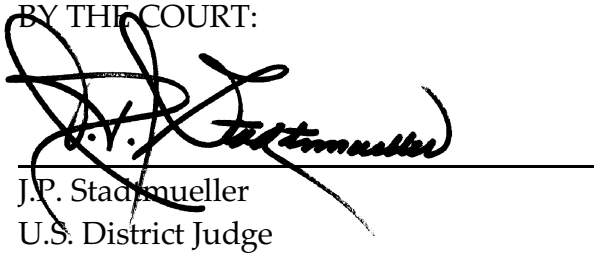
Accordingly,

IT IS ORDERED that Defendant Marcus A. Owens' objections to Magistrate Judge David E. Jones' order of November 4, 2016 (Docket #81) be and the same are hereby **OVERRULED**; and

IT IS FURTHER ORDERED that Magistrate Judge David E. Jones' order of November 4, 2016 (Docket #78) be and the same is **AFFIRMED**.

Dated at Milwaukee, Wisconsin, this 19th day of December, 2016.

BY THE COURT:



J.P. Stadtmueller
U.S. District Judge